A novel and robust security approach for authentication, integrity, and confidentiality of Lithium-ion Battery Management Systems

Luca Crocetti
Dept. of Information Engineering
University of Pisa
Pisa, Italy
luca.crocetti@unipi.it

Roberto Di Rienzo
Dept. of Information Engineering
University of Pisa
Pisa, Italy
roberto.dirienzo@unipi.it

Alessandro Verani
Dept. of Information Engineering
University of Pisa
Pisa, Italy
alessandro.verani@phd.unipi.it

Federico Baronti
Dept. of Information Engineering
University of Pisa
Pisa, Italy
federico.baronti@unipi.it

Roberto Roncella
Dept. of Information Engineering
University of Pisa
Pisa, Italy
roberto.roncella@unipi.it

Roberto Saletti
Dept. of Information Engineering
University of Pisa
Pisa, Italy
roberto.saletti@unipi.it

***Abstract*—Battery management systems (BMSs) play a critical and crucial role in ensuring the safety and the efficiency of the batteries. The increasing BMS complexity, the expanding interconnections between batteries and applications, and the introduction of cloud-based energy storage system structures have led to growing concerns about battery cybersecurity. For instance, the data exchange between the local and remote BMS parts can be exposed to cybersecurity attacks. Classic BMSs are not equipped with security mechanisms that are instead essential to protect their integrity and reliability and prevent serious consequences such as loss of data, equipment damage, and counterfeiting of battery components. This work highlights the importance of securing BMSs against cyber threats and discusses the current state of the art of cybersecurity in BMSs. The main outcome is the proposal of a novel and robust security approach to design a BMS able to prevent misuse and undesired manipulation of battery equipment and data. The proposed design approach can be used as enabling technology to support the application to the BMSs of the most diffused security mechanisms adopted by the state of the art as cybersecurity protections.**

***Index Terms*—Battery cybersecurity, battery authenticity, battery passport, electrical vehicle battery, battery counterfeiting protection, battery systems secure boot, secure battery management systems.**

I. Introduction

Li-ion batteries are nowadays largely diffused in many applications, such as electric vehicles and renewable energy storage systems, thanks to their high energy and power densities [1]. On the other hand, their working conditions should carefully be controlled to avoid accelerated degradation and hazardous conditions [2]. For this reason, Li-ion batteries are always equipped with an electronic control board called Battery Management System (BMS). Its main aim is to keep the battery in its Safe Operating Area (SOA) of voltage, temperature, and current [3]. Moreover, the BMS estimates and monitors the internal state variables of the battery and extracts useful battery information for the application, such as the State Of Charge (SOC) and the State Of Health (SOH) [4]. The BMS design relies on various architectures that differ in the distribution of the BMS functions among different hierarchical levels. The chosen architecture typically depends on the number of cells that compose the battery pack but also on the features required by the application such as flexibility, complexity, and computational power. The main control unit of a BMS is usually based on a microcontroller or a Field Programmable Gate Array (FPGA) if it requires low or high computation power and robustness, respectively [5].

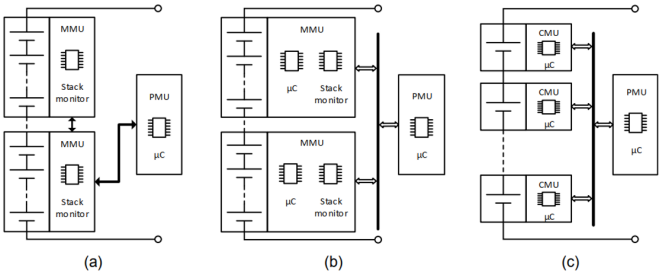

Fig. 1. Distributed topologies based on (a) MMUs with a stack monitor, (b) MMUs with a stack monitor and a microcontroller, and (c) Smart Cells. MMU, PMU, and CMU stand for Module Management Unit, Pack Management Unit and Cell Management Unit, respectively, while the symbol μC indicates a microcontroller.

The most used BMS architectures can be summarized in the three main topologies shown in Figure 1. The information and data concerning the cells and modules (i.e. a collection of cells) of the battery can be acquired and processed by a stack monitor and/or a microcontroller (denoted by the symbol μC) embedded within the Module Management Unit (MMU) or

the Cell Management Unit (CMU). The acquired quantities are transferred to the Pack Management Unit (PMU) via a communications bus such as the CAN-bus which is one of the most diffused. According to the BMS functionalities, the communication bus can also be used to transmit the commands from the PMU to the MMU and/or to the CMU, in order to manage the operations of the battery, e.g. charge cell equalization. In addition, other communication links can be integrated into the BMS to extend its functionalities, such as wireless links or other wired links to share the battery information with a remote server. For instance, Figure 2 shows the conceptual outline of a potential cloud-based BMS, derived from [6]. The cloud-based BMS is an advantageous solution to increase the computational and data storage capabilities of local BMSs. Moreover, more accurate and reliable battery algorithms can be developed and introduced in the cloud-based BMS to optimize battery use.

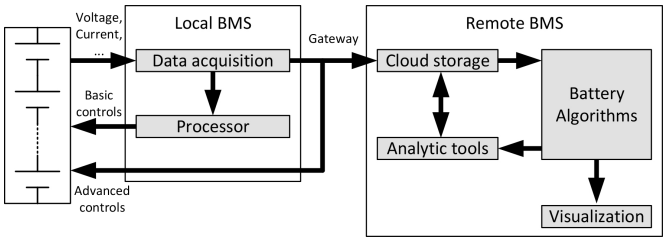

Fig. 2. Conceptual outline of a potential cloud-based BMS derived from [6].

However, the data exchange between the local BMS and the remote one can be exposed and susceptible to cybersecurity attacks. The attacks may aim at different purposes and their consequences can even be catastrophic, considering how the exchanged information affects battery operations and management. For instance, [7] and [8] report some cases of batteries that caught on fire or exploded because of the tampering of the information concerning the battery SOC and the consequent alteration of charge/discharge control operations.

Another severe threat in battery applications is the possibility to counterfeit or replace the components of batteries, such as the cells, modules, and BMS parts, with low-quality counterparts during maintenance and second-life application design. Such practices can seriously compromise the environment and the functionality of the battery and also introduce additional security breaches and leaks of critical information by means of backdoors or trojans in counterfeited firmware and software. Therefore, robust and proper security mechanisms must be integrated into the BMSs, in order to protect them and avoid or mitigate cyberattacks and their consequences.

In this work, the state of the art of the BMS cybersecurity mechanisms is analyzed. Then, a novel and robust security BMS scheme is proposed to implement both the literature and innovative functions and algorithms. In this way, the literature and innovative security solutions can be analyzed and compared to find the best security approaches that guarantee a good security level with a reasonable cost increase. The rest of the paper is organized as follows:

- Section II reports a cyber-physical perspective of BMSs in terms of cybersecurity, highlighting the main security threats and vulnerabilities;
- Section III describes the main security requirements and illustrates the proposed security scheme to protect BMS from the most critical security attacks;
- Finally, Section IV draws conclusions of this work by discussing the pros and cons of the presented solution, highlighting its advantages and increased robustness with respect to the state of the art of security measures for BMSs.

II. Cyber-physical security overview of Battery Management Systems

Works [7]–[9] give a general overview of the security weaknesses and attacks that can be issued against a BMS, while [10] is more focused on the physical protection of BMSs. In particular, it proposes a solution for the anti-counterfeiting protection of batteries. Some other security solutions can be found in [11] which addresses the security evaluation of wireless BMSs (WBMSs). These works provide a complete picture of the state of the art of cybersecurity topics for battery applications. The security vulnerabilities analysis and the corresponding possible countermeasures are summarized in Section II-A and II-B, respectively.

In order to draw out a comprehensive security perspective of BMSs, a layered approach similar to the one presented in [7] can be applied to the architectures illustrated in Figure 1 and Figure 2. Hence the battery system is divided into Physical, BMS, Application, and Network layers. The physical layer includes the battery cells, modules, and the surrounding circuitry including the CMU and MMU hardware. The CMU and MMU software are considered part of the BMS layer together with the PMU hardware and software components. The physical and BMS layers perform the functions of monitoring, protecting, estimating, performance maximizing, and reporting the battery state to users and external devices. The Application layer extends and improves the BMS functionalities for a specific application. Finally, the Network layer is applied only to battery systems equipped with remote connections and includes interactions with external entities.

A. Security threats, vulnerabilities, and attacks

Cybersecurity threats in BMSs and the corresponding attacks can be individuated at:

- **Physical layer**. The main attack of this level concerns the counterfeiting of original battery equipment, by replacement or substitution with low-quality or damaged ones. This attack requires the physical access of the battery and then it is usually carried out during maintenance or in second-life applications. The second-life battery application is a very interesting approach because allows us to reuse the exhausted vehicle battery (i.e. battery with about $80\,\%$ SoH [12]) in applications with lower power

request. Typical second-life applications are the smart grids, as shown in [10], and battery swapping stations as reported in [7]. Degraded and flawed battery equipment can seriously compromise the target application and lead to several undesired and dangerous effects.

- **BMS layer**. At this layer, a malicious entity, or the battery producer itself, can target both hardware and software components by introducing backdoors, trojans, and counterfeited firmware. These attacks aim to disrupt the availability of BMS services (e.g., by implementing a typical Denial-of-Service, DoS, attack) and to access safety-critical information, such as SOC and SOH. For instance, a DoS attack can be issued on the CAN-bus (i.e. a multi-master broadcast link with automatic arbitration and message priority) with the injection of highest priority messages that override the lower priority ones occupying the bus.
- **Application layer**. At this level, the most typical cyberattacks aim at violating the availability, integrity, and confidentiality of data. For instance, the CAN-bus can once again be vulnerable to confidentiality attacks because it does not include any security algorithm for the privacy of data but only a Cyclic Redundancy Check (CRC) value to evaluate the consistency of messages.
- **Network layer**. This layer is affected by the same cybersecurity attacks and vulnerabilities of the Application layer targeting the violation of the same data security properties. Moreover, the attacker can conduct more advanced attacks such as the Man-In-The-Middle (MITM) one.

In addition to the vulnerabilities described in the list above, more sophisticated attacks can be implemented starting from one of the indicated layers and propagating to the other ones. These attacks are usually called "cross-layer" attacks and are more difficult to detect and counter [7].

B. State of the Art of security measures

The state of the art of cybersecurity solutions and mechanisms for BMSs counts two main protection strategies [7]–[11], [13]. The first one protects the battery equipment, in particular the battery cells and modules, by ensuring its origin. The second one aims to protect the BMS data by ensuring its authenticity, integrity, and its confidentiality.

Blümke et al. in [10] introduce the concept of a battery passport, a certificate of authenticity for a battery, including all the information related to its life cycle from the production phase to the disassembly of the vehicle and its recycling in second-life applications. Such passport should be regulated also by law and relayed on the generation of a unique and unclonable hardware identifier of the battery (or its components) by exploiting the Physically Unclonable Functions (PUFs). PUFs are a computational and financially inexpensive alternative to store cryptographic keys or identifiers in non-volatile memory [14].

The authors of [7]–[9], [11], [13], instead, focus on data protection by introducing specific solutions for wired and wireless links. For instance, they propose the employment of blockchain technologies in WBMSs and the adoption of typical cybersecurity algorithms for the encryption of data on traditional wired links, such as the CAN-bus. Such solutions aim to guarantee the authenticity of the data sources and their integrity, especially with blockchain technologies. The blockchain exploits digital signature mechanisms, hash functions, and the confidentiality of data in case of data encoding with symmetric-key ciphers. Moreover, [9] proposes the utilization at the network level of traditional cybersecurity protocols and functions such as TLS/SSL, SSH, hash functions, and encryption algorithms.

Table I summarizes the security services that are currently by the state of the art:

TABLE I
SECURITY SERVICES OFFERED BY THE STATE OF THE ART FOR PROTECTION OF BMSS.

Security mechanism/solution	Security service/protected assets
Battery passport	Authentication of BMS components origin
Blockchain technology	Authentication of BMS data source Integrity of BMS data
Traditional cybersecurity algorithms (e.g.: data encryption of CAN packets)	Confidentiality of BMS data

Anyway, such solutions may present significant drawbacks. For instance, the adoption of blockchain technologies requires the usage of big memories and storage resources to store all transactions (i.e. exchanged data) over time. A communication overhead can be introduced by the encryption with the Advanced Encryption Standard (AES) cipher [13] of CAN-bus packets, because the payload of a CAN message is at most 64 bits, while the AES algorithm encrypts data in blocks of 128 bits, hence requiring at least two CAN packets. In addition, the usage of AES requires us to address the typical problems related to the exchange and the establishment of cryptographic keys for symmetric-key ciphers.

III. SECURITY MEASURES FOR BATTERY MANAGEMENT SYSTEMS

The main security requirements for the protection of BMS assets are illustrated in Section III-A. They are derived starting from the security perspective including the vulnerabilities analysis and the state of the art of security mechanisms described in Section II. These requirements are the basis on which a novel and robust security scheme that addresses them is proposed in Section III-B. Basing on the security perspective including the vulnerabilities analysis and the state of the art of security mechanisms described in Section II, the main security requirements for the protection of BMS assets are illustrated in Section III-A and are consequently used to present in Section III-B a novel and robust security scheme able to address them.

A. Overall security requirements, features and primitives

The main security requirements for BMSs concern anti-counterfeiting protections and measures for the authentication of data sources and data integrity. The confidentiality of data,

instead, is important but has a lower priority. It is required only in cases in which sensitive user and battery data are exchanged with the remote server. For this purpose, the use of a mechanism for the generation of a unique, unpredictable, and unclonable identifier becomes mandatory. The identifier supports the battery passport preventing the counterfeit of BMS equipment. On the other hand, typical security solutions suggest the employment of digital signature algorithms and hash functions to prove the authenticity and the integrity of data, respectively. For example, the blockchain technologies proposed in [7], [8], [11] rely on the Elliptic Curve Digital Signature Algorithm, ECDSA [15], and the Secure Hashing Algorithm (SHA) such as the SHA2-256 [16].

The usage of ECDSA, which is based on Elliptic Curve Cryptography (ECC), is strongly recommended if compared to the integer factorization functions, i.e. the Rivest-Shamir-Adleman (RSA, [15]) algorithm. In fact, the ECDSA can provide the same level of security as RSA using a lower amount of resources (smaller keys, smaller storage space, ...) [19]. The SHA2, instead, represents the de-facto standard for data integrity and the use of 256-bit digests (i.e. SHA2-256) provides the minimum security level considered robust and sufficient, as indicated in [20]. Indeed, the analysis of the security strength of hash algorithms presented in [20] reveals that the SHA2-256 function provides a security level of 128 bits which is the minimum security level acceptable in security applications through 2031 and beyond. The same security lever can be obtained with the SHA-3-256 function. It is based on the SHA-3 algorithm [17], which is less diffused than SHA2 and typically requires a greater amount of logic resources [20]. Finally, the AES [18] represents the de-facto standard concerning confidentiality protection through encryption. It is widely accepted for symmetric-key encryption applications as suggested in [13]. In addition, AES is a primitive employed in the higher-level security protocols such as TSL/SSL and SSH proposed in [9].

In conclusion, the main security requirements and primitives to protect BMSs from the most critical security vulnerabilities can be summarized with the list illustrated in Table II.

TABLE II
SECURITY REQUIREMENTS, PRIMITIVES, AND SERVICES FOR BMS PROTECTION.

Security requirement	Method (or algorithm)	Security service
Unique, unclonable ID generator	PUF	Anti-counterfeiting protection
Digital signature	ECDSA	Data authentication
Hash function	SHA2	Data integrity
Encryption	AES	Data confidentiality

B. A novel and robust security scheme for BMS

Our solution for the protection of BMSs relies on the integration of a secure boot routine based on a hardware Root-of-Trust (RoT) inside the tiniest atomic element of the BMS equipment. The atomic adjective refers to the purpose of addressing the BMS element that can be considered sealed and typically cannot be physically tampered by an external attacker, and all its components correspond to the original ones. Based on this and referring to Figure 1, the secure boot routine can be performed by integrating a unit dedicated to the generation (and/or storage) of a unique and unclonable identifier within the MMU/CMU. The identifier can be used as a root key for the generation/derivation of additional cryptographic keys. Moreover, one or more cryptographic hardware co-processors, Non-Volatile Memories (NVMs), and One-Time-Programmable (OTP) memories can be assembled into the MMU/CMU to easily implement the security functions and algorithms. Hence, the outline of the proposed Secure MMU/CMU unit is drawn out in Figure 3, including the other hardware equipment used for the typical BMS functionalities.

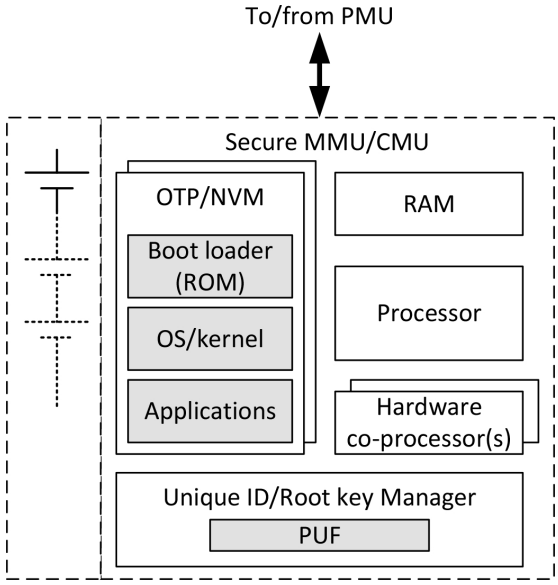

Fig. 3. Outline of proposed Secure MMU/CMU.

With reference to Figure 3, the OTP/NVM resources are used to store the multiple stages of the boot and software code (i.e. the bootloader ROM, the second boot stage, and so on), while the *Unique ID/Root key Manager* unit is based on PUF and generates a unique identifier or root key for each different chip. This last element and the OTP/NVM memory store the first boot stage and constitute the hardware part of the RoT. It is the basis for the secure boot routine, and, by definition, it is considered implicitly trusted and secure. Therefore, the device dedicated to the boot, which can be the processor or the hardware co-processor, moves the code of the first boot stage from the OTP/NVM to the RAM, then it verifies its authenticity with the digital signature and its integrity. If all the checks are successful, then the second boot stage can be performed with the loading and execution of the runtime code and applications.

The availability of a PUF is generally not strictly required to build a secure boot routine. However, it allows the generation of a unique identifier for the battery passport implementation.

In addition, the identifier can be used as a root cryptographic or to derive cryptographic keys that can be used to encrypt the content of the OTP/NVM memory. In this way, the secure boot routine and the related security assets become more robust from a security point of view, and the content of the OTP/NVM is different for each chip. An attacker that is able to disclose the OTP/NVM content of one chip does not have information on the content of the OTP/NVM of the other chips [22]. On the other hand, the boot device must decrypt the bootloader image when loading it in the RAM increasing the required computational effort.
In addition, the first boot stage code should be stored in an OTP, while the other boot stages' code and the code of the remaining software stack can be stored in NVM resources. This is not strictly required, but it is highly suggested to ensure that the RoT assets (including the first boot stage), will not be modified during the life cycle of the battery, as they will always constitute the trusted and secure anchor released by the chip manufacturer. Instead, the usage of reprogrammable NVM, to store the other software code sections, gives the possibility to update the firmware afterward. Moreover, the NVM resources can be used to store significant information about the battery during its life cycle, even in an encrypted format, contributing to the management of the battery passport.

The additional security functions and algorithms require a computational load that could not be compatible with the microcontroller usually employed in MMU/CMU. For example, the computational load required to perform the ECDSA algorithm used for the verification of the boot code is intensive and takes up to some seconds using a Broadcom BCM2837B0 chip running @ $1.4\,\mathrm{GHz}$ as demonstrated in [23]. For these reasons, an upgrade of the MMU/CMU microcontroller and/or dedicated hardware co-processors is required. In order to improve and strengthen the security level, the second option has to be preferred because, for instance, embedded hardware mechanisms can directly manage the access to the cryptographic keys from the *Unique ID/Root key Manager* or the boot code, allowing their utilization to the software applications but without revealing their value or regulating their usage according to different privilege levels. This approach prevents hacked software from violating security-critical assets. Therefore, the integration of hardware cryptographic co-processing unit(s) has to be considered fundamental, and at least acceleration engine(s) for the ECC/ECDSA operations and SHA2 functions should be included to verify, respectively, the authenticity and integrity of the boot code.

All the key elements illustrated so far consent to implement a secure boot routine allowing us to realize a local Chain-of-Trust. The Chain-of-Trust is internal to the Secure MMU/CMU but it can be extended also to the other layers of the BMS. Indeed, the first boot stage verifies the RoT and enables the extension of the security zone from the RoT to the second boot stage. Then, the verified second boot stage can in its turn verify the other software code sections, and so on, extending step by step the security zone up to all the MMU/CMU elements. In addition, the aforementioned features can also be applied to firmware updates. The secure boot sequence is interrupted and the system is moved into a secure and dedicated recovery state that is accessible only to authorized entities if any step of the local Chain-of-Trust fails. In this case, for instance, additional resources supporting the recovery state can be integrated, in accordance with the security requirements and specifications released by the National Institute of Standards and Technology (NIST) about the resiliency of digital platforms firmware [21].
Once the local Chain-of-Trust is established, it can be extended to the other BMS components also. For instance, the Chain-of-Trust can be extended to the PMU with the integration of similar resources for the execution of a secure boot routine in it. Similarly, the security zone can be extended to the higher layers up to the application one and even to the execution of secure routines up to the network layer. Indeed, if both the MMU/CMU and the PMU are secure, the whole BMS will be considered secure. Consequently, if proper security mechanisms ensure the reliability of the BMS applications from a security perspective, every BMS joining the same network can be considered a trusted and secure node. Hence, the security protections can be extended to the network level with the goal to identify and counteract attacks from the external. At the same time, if any of the steps required for the construction of the Chain-of-Trust across the layers fail in a node, that node can be considered insecure and excluded from the network.
In conclusion, the elements presented and discussed here that lead to the realization of secure MMU/CMUs can be used as integrating and enabling technology for the implementation of general security solutions found in the state of the art. For example, the availability of secure MMU/CMUs enables not only the battery passport, supported by the *Unique ID/Root key Manager* and secure NVM resources but also the blockchain technologies and the TSL/SSL and SSH protocols. In fact, these techniques rely on security primitives such as ECDSA and SHA2 which are usually supported by cryptographic hardware co-processors. Instead, other security algorithms, such as the AES for the encryption of CAN messages, can be easily implemented in software assuming the extension of the secure zone up to the MMU/CMU processor. This approach would allow the reduction of hardware costs.

IV. Conclusions

This work investigates and reports the state of the art of the most critical security vulnerabilities of BMSs and batteries. A novel and robust security solution is presented to tackle the critical security vulnerabilities in electric vehicle batteries with a particular focus on their reuse in second-life applications. The proposed solution relies on a secure boot routine and a hardware RoT that provide highly-qualified and complete security protection in terms of anti-counterfeiting, authentication, and integrity of BMS equipment and data. Moreover, the solution proposed here gives the possibility to build a Chain-of-Trust able to protect all the BMS components.

The proposed security BMS architecture tries to make the most of the already available components of a classic BMS minimizing the additional dedicated logic resources and then the BMS security cost. At the same time, our solution can easily be improved to support and facilitate the integration of higher-level and more complex security mechanisms and protocols proposed in the literature.

Future works will focus on a deeper definition and characterization of the proposed approach for the organization (and eventually the isolation) of the non-security-related and security-related components of BMS in different security zones (or domains), the security assets, and the related resources, by targeting the best components in terms of trade-off among security strength, features, cost, performance, and power consumption. Also extensions of the proposed solution will be considered, for instance, for addressing the cybersecurity requirements in cloud-based BMS that may use Ethernet (or Automotive Ethernet) links [7] for high-volume traffic of data in short time intervals and can be protected by integrating embedded hardware accelerators for the AES-based Media Access Control Security (MACsec) standard [24], such as the one proposed in [25].

ACKNOWLEDGMENT

This work was partially supported by the Italian Ministry of University and Research (MUR) through the project CN4 - CN00000023 of the Recovery and Resilience Plan (PNRR) program, grant agreement no. I53C22000720001, and in the framework of the FoReLab project (Departments of Excellence).

REFERENCES

[1] A. Dutta, S. Mitra, M. Basak, and T. Banerjee, "A comprehensive review on batteries and supercapacitors: Development and challenges since their inception," Energy Storage, vol. 5, article e339, 2023.

[2] C. Feng and X. Yang, "Explosion mechanism and prevention of lithium-ion batteries," 2019 IEEE Sustainable Power and Energy Conference (iSPEC), Beijing, China, November 2019, pp. 969-974.

[3] H.A. Gabbar, A.M. Othman, and M.R. Abdussami, "Review of Battery Management Systems (BMS) Development and Industrial Standards." Technologies 2021, vol.9, 28, 2021.

[4] R. Morello, R. Di Rienzo, R. Roncella, R. Saletti, R. Schwarz, V.R.H. Lorentz, E.R.G. Hoedemaekers, B. Rosca, F. Baronti, "Advances in Li-Ion Battery Management for Electric Vehicles," IECON 2018 - 44th Annual Conference of the IEEE Industrial Electronics Society, Washington, DC, USA, 2018, pp. 4949-4955.

[5] A. Verani, G. Fieramosca, A. Colicelli, R. Di Rienzo, R. Saletti, R. Roncella, R. Schwarz, V.R.H. Lorentz, F. Baronti, "FPGA Accelerator for Battery Management Systems in Safety-Critical Applications," 2020 2nd IEEE International Conference on Industrial Electronics for Sustainable Energy Systems (IESES), Cagliari, Italy, 2020, pp. 261-266.

[6] M. K. Tran, S. Panchal, T. D. Khang, K. Panchal, R. Fraser, and M. Fowler, "Concept review of a cloud-based smart battery management system for lithium-ion batteries: Feasibility, logistics, and functionality,". Batteries, vol. 8, issue 2, article 19, 2022.

[7] A. B. Lopez, K. Vatanparvar, A. P. Deb Nath, S. Yang, S. Bhunia and M. A. Al Faruque, "A security perspective on battery systems of the Internet of Things," Journal of Hardware and Systems Security, vol. 1, pp. 188–199, April 2017.

[8] T. Kim, J. Ochoa, T. Faika, H. A. Mantooth, J. Di, Q. Li and Y. Lee, "An overview of cyber-physical security of battery management systems and adoption of blockchain technology," IEEE Journal of Emerging and Selected Topics in Power Electronics, vol. 10, issue 1, pp. 1270–1281, February 2020.

[9] S. Kumbhar, T. Faika, D. Makwana, T. Kim, and Y. Lee, "Cybersecurity for battery management systems in cyber-physical environments," In 2018 IEEE Transportation Electrification Conference and Expo (ITEC), pp. 934-938, June 2018.

[10] J. Blümke, and H. J. Hof, "Authentic batteries: a concept for a battery pass based on PUF-enabled certificates," In SECURWARE 2022: The Sixteenth International Conference on Emerging Security Information, Systems and Technologies, pp. 76–81), 2022.

[11] T. Faika, T. Kim, J. Ochoa, M. Khan, S. W. Park and C. S. Leung, "A blockchain-based internet of things (IoT) network for security-enhanced wireless battery management systems," In 2019 IEEE industry applications society annual meeting, pp. 1–6, September 2019.

[12] E. Hossain, D. Murtaugh, J. Mody, H. M. R. Faruque, M. S. Haque Sunny and N. Mohammad, "A Comprehensive Review on Second-Life Batteries: Current State, Manufacturing Considerations, Applications, Impacts, Barriers & Potential Solutions, Business Strategies, and Policies," in IEEE Access, vol. 7, pp. 73215-73252, 2019.

[13] G. Zimmer, "Wireless battery management systems highlight industry's drive for higher reliability," Linear Technology, February 2017.

[14] G. E. Suh and S. Devadas, "Physical unclonable functions for device authentication and secret key generation," Proceedings of the 44th annual design automation conference, pp. 9–14, 2017.

[15] NIST standard, "Digital signature standard (DSS)," Federal Information Processing Standards Publication 186-5, NIST, February 2023.

[16] NIST standard, "Secure hash standard," Federal Information Processing Standards Publication 180-4, NIST, August 2015.

[17] NIST standard, "SHA-3 standard: Permutation-based hash and extendable-output functions," Federal Information Processing Standards Publication 202, NIST, August 2015.

[18] NIST standard, "Advanced Encryption Standard (AES)," Federal Information Processing Standards Publication 197, NIST, November 2001.

[19] S. Di Matteo, L. Baldanzi, L. Crocetti, P. Nannipieri, L. Fanucci, and S. Saponara, "Secure elliptic curve crypto-processor for real-time IoT applications," Energies, vol. 14, issue 15, article 4676, 2021.

[20] P. Nannipieri, M. Bertolucci, L. Baldanzi, L. Crocetti, S. Di Matteo, F. Falaschi, L. Fanucci, and S. Saponara, S., "SHA2 and SHA-3 accelerator design in a 7 nm Technology within the european processor initiative," Microprocessors and Microsystems, vol. 87, article 103444, 2021.

[21] NIST standard, "Platform Firmware Resiliency Guidelines," Special Publication 800-193, NIST, 2017. https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-193.pdf (accessed on 24 February 2023).

[22] M. Deutschmann, L. Iriskic, S. L. Lattacher, M. Münzer, and O. Tomshchuk, "A PUF based hardware authentication scheme for embedded devices," Technical report, Technikon Forschungs-und Planungsgesellschaft mbH, Burgplatz, 2018. https://technikon.com/wp-content/uploads/2019/12/White-Paper-on-PUF-Based-HW-Authentication.pdf (accessed on 24 February 2023).

[23] L. Baldanzi, L. Crocetti, S. Di Matteo, L. Fanucci, S. Saponara, and P. Hameau, "Crypto accelerators for power-efficient and real-time on-chip implementation of secure algorithms," In 2019 26th IEEE International Conference on Electronics, Circuits and Systems (ICECS), pp. 775-778, November 2019.

[24] IEEE, "IEEE Standard for Local and metropolitan area networks-Media Access Control (MAC) Security," IEEE 802.1AE-2018 (2018).

[25] B. Carnevale, F. Falaschi, L. Crocetti, H. Hunjan, S. Bisase, and L. Fanucci, "An implementation of the 802.1 AE MAC Security Standard for in-car networks," In 2015 IEEE 2nd World Forum on Internet of Things (WF-IoT), pp. 24-28, December 2015.